INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

C-tableaux

Calogero G. Zarba

N° 5229

June 2004

Thème SYM

Rapport de recherche

ISRN INRIA/RR--5229--FR+ENG

ISSN 0249-6399

C-tableaux

Calogero G. Zarba

Thème SYM — Systèmes symboliques
Projet CASSIS

Rapport de recherche n° 5229 — June 2004 — 31 pages

Abstract: The Nelson-Oppen combination method combines decision procedures for first-order theories satisfying certain conditions into a single decision procedure for the union theory. The method is restricted to the combination of stably infinite theories over disjoint signatures.

In this report we present *C-tableaux*, an extension of Smullyan tableaux that generalizes the Nelson-Oppen method to the combination of arbitrary universal theories, not necessarily stably infinite and not necessarily over disjoint signatures. C-tableaux are sound and complete, but not terminating in general.

Although C-tableaux do not provide a decidability result in general, in this report we describe two approaches that can be used in order to obtain decidability results using C-tableaux. Using the first approach, we are able to obtain a decidability result when combining theories that share the dense orders. Using the second approach, we are able to obtain a decidability result when combining theories whose union is stably finite.

Key-words: Automated deduction, Decision procedures, Combination, Tableaux.

Unité de recherche INRIA Lorraine
LORIA, Technopôle de Nancy-Brabois, Campus scientifique,

C-tableaux

Résumé : La méthode de combinaison de Nelson-Oppen permet de combiner des procédures de décision pour des théories du premier ordre satisfaisant certaines conditions de manière à obtenir une procédure de décision pour l'union des théorie. La méthode est restreinte à la combinaison de théories stable-infinies sur des signatures disjointes.

Dans ce rapport, nous présentons les C-tableaux, une extension des tableaux de Smullyan qui généralise la méthode de Nelson-Oppen à la combinaison de théories arbitraires universelles, pas nécessairement stable-infinies et pas nécessairement à signatures disjointes. La méthode des C-tableaux est correcte et complète, mais ne termine pas en général.

Bien que les C-tableaux ne fournissent pas un résultat de décidabilité en général, nous décrivons dans ce rapport deux approches les utilisant qui permettent d'obtenir des résultats de décidabilité. En employant la première approche, nous pouvons obtenir un résultat de décidabilité quand nous combinons des théories qui partagent les ordres denses. En employant la deuxième approche, nous pouvons obtenir un résultat de décidabilité quand nous combinons des théories dont l'union est stable-finie.

Mots-clés : Déduction automatique, Procédures de décision, Combinaison, Tableaux.

Contents

1 Introduction

In many applications of automated reasoning one has often to detect the satisfiability of logical formulae spanning several different domains. Thus, it is important to build frameworks for combining the different specialized reasoners for the single domains into a general-purpose reasoner.

The most successful and well-known combination method was invented in 1979 by Nelson and Oppen [7]. Given two theories T_1 and T_2 satisfying certain conditions, their method combines the available decision procedures for T_1 and T_2 into a decision procedure for the satisfiability of quantifier-free formulae in the union theory $T_1 \cup T_2$. In order to be applicable, the Nelson-Oppen method requires that the component theories T_1 and T_2 satisfy the following conditions:

- the theories T_1 and T_2 must be stably infinite;[1]
- the signatures of T_1 and T_2 must be disjoint.

In this report we address the problem of lifting both the stably infiniteness and the disjointness restriction. To solve this problem, we introduce *C-tableaux*, an extension of Smullyan tableaux [1, 10] which generalizes the Nelson-Oppen combination method to the union of arbitrary universal theories, not necessarily stably infinite and not necessarily over disjoint signatures.

C-tableaux use as black boxes decision procedures P_1 and P_2 for the satisfiability of quantifier-free formulae in theories T_1 and T_2 in order to provide a sound and complete method with respect to the *unsatisfiability* of quantifier-free formulae in the combined theory $T_1 \cup T_2$. Soundness means that if there exists a C-tableau proof that a formula is unsatisfiable in the combined theory, then the formula is indeed unsatisfiable. Completeness means that if a formula is unsatisfiable in the combined theory, then there exists a C-tableau proof that demonstrates the unsatisfiability.

In general, C-tableaux are not terminating. In other words, a procedure based on C-tableaux may run forever if it receives as input a formula that is satisfiable in the combined theory. Note that nontermination is exactly what is expected because the general problem targeted by C-tableaux is undecidable.

Although in general C-tableaux do not provide a decidability result, there are particular instances of combination problems where C-tableaux do yield a decision procedure for the combined theory. Indeed, there are two main approaches that can be used in order to obtain a decidability result using C-tableaux.

The first approach consists of employing, depending upon the specific component theories at hand, suitable restrictions to the tableau rules that enforce termination without sacrificing completeness.

Using this approach, we show that C-tableaux provide a decidability result when combining theories that share the dense orders. The theory of dense orders models a predicate

[1] A theory is stably infinite if every quantifier-free formula is satisfiable in T if and only if it is true in an infinite model of T.

symbol $<$ as a linear order that is dense in the following sense: For every two elements x, y, if $x < y$ then there exists an element z between x and y, that is, $x < z$ and $z < y$. Examples of domains that are densely ordered include the set of rational numbers and the set of real numbers.

The second approach consists of finding a semi-decision procedure that is sound and complete for the ***satisfiability*** of quantifier-free formulae in $T_1 \cup T_2$. Note that C-tableaux are a semi-decision procedure that is sound and complete for the ***unsatisfiability*** of quantifier-free formulae in $T_1 \cup T_2$. Therefore, given a quantifier-free formula φ, we can run the two semi-decision procedures in parallel, and the first one that stops will tell us whether φ is $(T_1 \cup T_2)$-satisfiable or not.

Using the second approach, we are able to obtain a decidability result when combining universal theories T_1, T_2 whose union $T_1 \cup T_2$ is stably finite.[2]

1.1 Related work

Tinelli and Ringeissen [13] presented a generalization of the Nelson-Oppen combination method for theories whose signatures may not be disjoint. Their method is restricted to pairs of what they call ***N-O combinable*** theories. Roughly speaking, examples of pairs of N-O combinable theories are those that share constructors, and also "agree" on the shared constructors. Given a pair $\langle T_1, T_2 \rangle$ of N-O combinable theories, Tinelli and Ringeissen's method yields a semi-decision procedure with respect to the satisfiability of constraints in the union theory $T_1 \cup T_2$.

Tinelli [11] introduced a multi-theory free-variable tableau calculus in which the foreground reasoner interacts with two background reasoners. His method is based on a specialized version of the Craig interpolation lemma.

Ghilardi [2] presented another generalization of the Nelson-Oppen combination method for theories whose signatures may not be disjoint. His method is restricted to pairs of theories $\langle T_1, T_2 \rangle$ for which there is a theory T_0 such that both T_1 and T_2 are what Ghilardi calls T_0-***compatible*** theories. As an example, the theory of rational linear arithmetic and the theory of total orders endowed with a strict monotonic function f are T_0-compatible, with T_0 being the theory of total orders. Ghilardi's method yields a semi-decision procedure with respect to the unsatisfiability of constraints in the union theory $T_1 \cup T_2$, but it can provide a decidability result if the theory T_0 is locally finite.

1.2 History of C-tableaux.

C-tableaux were originally presented in [14], and then later improved in [15]. The decidability result for the combination of theories sharing dense orders was first obtained in [17]. The decidability result for the combination of theories whose union is stably finite was first obtained in [16].

[2] A theory is stably finite if every quantifier-free formula is satisfiable in T if and only if it is true in a finite model of T.

1.3 Organization of the report.

The report is organized as follows. In Section 2 we introduce some preliminary notions that will be used in what follows. In Section 3 we describe the Nelson-Oppen combination method, and in Section 4 we describe C-tableaux. In Sections 5 we state and prove the Combination Theorem, a fundamental model-theoretic result that forms the basis of the correctness of combination methods. In Section 6 we prove the soundness and completeness of C-tableaux. In section 7 we address the problem of making C-tableaux efficient. In Section 8 we show how to obtain a decidability result when combining theories that share up to a finite number of constant symbols. In Section 9 we show how to obtain a decidability result when combining theories that share the dense orders. In Section 10 we show how to obtain a decidability result when combining theories whose union is stably finite. Finally, in Section 11 we draw conclusions from our work.

2 Preliminaries

2.1 Syntax

A ***signature*** Σ consists of a set Σ^{C} of constant symbols, a set Σ^{F} of function symbols, and a set Σ^{P} of predicate symbols.

Given a set V of variables, we denote with $\mathit{Terms}(\Sigma, V)$ the set of terms built from the variables in V and the symbols in Σ. An element of $\mathit{Terms}(\Sigma, V)$ is a Σ-***term***. $\mathit{Terms}(\Sigma)$ stands for $\mathit{Terms}(\Sigma, \emptyset)$.

A Σ-***atom*** is either an expression of the form $P(t_1, \dots, t_n)$, where $P \in \Sigma^{\mathrm{P}}$ and $t_1, \dots, t_n$ are Σ-terms, or an expression of the form $s = t$, where $=$ is the equality logical symbol and s, t are Σ-terms, or one of the symbols true, false. Σ-***formulae*** are constructed by applying in the standard way the connectives $\neg$, $\wedge$, $\vee$, $\rightarrow$ and the quantifiers $\forall, \exists$ to Σ-atoms. Σ-***literals*** are Σ-atoms or their negations. Σ-***sentences*** are Σ-formulae with no free variables.

When Σ is irrelevant or clear from the context, we will simply write atom, formula, literal, and sentence in place of Σ-atom, Σ-formula, Σ-literal, and Σ-sentence.

If t is a term, $\mathit{vars}(t)$ denotes the set of variables occurring in t. If φ is a formula, $\mathit{vars}(\varphi)$ denotes the set of free variables occurring in φ. If Φ is a set of terms or a set of formulae, $\mathit{vars}(\Phi) = \bigcup_{\varphi \in \Phi} \mathit{vars}(\varphi)$.

For convenience, we identify conjunction of formulae $\varphi_1 \wedge \cdots \wedge \varphi_n$ with the set $\{\varphi_1, \dots, \varphi_n\}$, and we abbreviate the literal $\neg(x = y)$ with $x \neq y$.

2.2 Semantics

Definition 1. Let Σ be a signature. A Σ-INTERPRETATION $\mathcal{A}$ with domain A over a set V of variables is a map which interprets

- each variable $x \in V$ as an element $x^{\mathcal{A}} \in A$;
- each constant $c \in \Sigma^{\mathrm{C}}$ as an element $c^{\mathcal{A}} \in A$;

- each function symbol $f \in \Sigma^{\mathrm{F}}$ of arity n as a function $f^{\mathcal{A}} : A^n \to A$;
- each predicate symbol $P \in \Sigma^{\mathrm{P}}$ of arity n as a subset $P^{\mathcal{A}}$ of A^n. □

Unless otherwise specified, we use the convention that calligraphic letters $\mathcal{A}$, $\mathcal{B}$, ... denote structures, and that the corresponding Roman letters A, B, ... denote the domains of the structures.

Let $\mathcal{A}$ be a Σ-interpretation over a set V of variables. For a term $t \in \mathit{Terms}(\Sigma, V)$, we denote with $t^{\mathcal{A}}$ the evaluation of t under the interpretation $\mathcal{A}$. Similarly, we denote with $\varphi^{\mathcal{A}}$ the truth-value of the formula φ under the interpretation $\mathcal{A}$. If T is a set of Σ-terms over V, we denote with $T^{\mathcal{A}}$ the set $\{t^{\mathcal{A}} : t \in T\}$.

A sentence φ is *satisfied* by an interpretation $\mathcal{A}$ if it evaluates to true under $\mathcal{A}$. A Σ-formula φ over a set V of variables is:

- *valid*, if it is satisfied by all Σ-interpretations over V;
- *satisfiable*, if it satisfied by some Σ-interpretation over V;
- *unsatisfiable*, if it is not satisfiable.

Let $\mathcal{A}$ be an Ω-structure over some set U of variables. For a subset Σ of Ω and a subset V of U, we denote with $\mathcal{A}^{\Sigma,V}$ the Σ-interpretation over U obtained by restricting $\mathcal{A}$ to interpret only the symbols in Σ and the variables in U. In particular, $\mathcal{A}^{\Sigma}$ stands for $\mathcal{A}^{\Sigma,\emptyset}$.

Definition 2. Let $\mathcal{A}$ and $\mathcal{B}$ be Σ-interpretations over V. A QUASI-EMBEDDING h of $\mathcal{A}$ into $\mathcal{B}$ is a function $h : A \to B$ such that

- $h(u^{\mathcal{A}}) = u^{\mathcal{B}}$ for each constant or variable u in $\Sigma^{\mathrm{C}} \cup V$;
- $h(f^{\mathcal{A}}(a_1, \ldots, a_n)) = f^{\mathcal{B}}(h(a_1), \ldots, h(a_n))$, for each n-ary function symbol f in Σ^{F} and for each $a_1, \ldots, a_n$ in A;
- $(a_1, \ldots, a_n) \in P^{\mathcal{A}}$ if and only if $(h(a_1), \ldots h(a_n)) \in P^{\mathcal{B}}$, for each n-ary predicate symbol P in Σ^{P} and for each $a_1, \ldots, a_n$ in A.

An EMBEDDING of $\mathcal{A}$ into $\mathcal{B}$ is an injective quasi-embedding h of $\mathcal{A}$ into $\mathcal{B}$.
An ISOMORPHISM of $\mathcal{A}$ into $\mathcal{B}$ is a bijective quasi-embedding h of $\mathcal{A}$ into $\mathcal{B}$. □

We write $\mathcal{A} \cong \mathcal{B}$ to indicate that there exists an isomorphism of $\mathcal{A}$ into $\mathcal{B}$.

Proposition 3. *Let $\mathcal{A}$ and $\mathcal{B}$ be Σ-interpretations over V, and assume that $\mathcal{A} \cong \mathcal{B}$. Then $\varphi^{\mathcal{A}} = \varphi^{\mathcal{B}}$, for each Σ-formula φ such that $\mathit{vars}(\varphi) \subseteq V$.* □

Proposition 4 ([5]). *Let $\mathcal{A}$ and $\mathcal{B}$ be two interpretations, and let T be a universal theory such that $\mathcal{B}$ is a T-interpretation. Assume that there exists an embedding of $\mathcal{A}$ into $\mathcal{B}$. Then $\mathcal{A}$ is also a T-interpretation.* □

Theorem 5 (Herbrand). *Let Φ be a set of universal Σ-formulae, and let $V = \mathit{vars}(\Phi)$. Assume that $\Sigma^{\mathrm{C}} \cup V \neq \emptyset$. Then Φ is satisfiable if and only if there exists an interpretation $\mathcal{A}$ satisfying Φ such that $A = [\mathit{Terms}(\Sigma, V)]^{\mathcal{A}}$.* □

2.3 Theories

Definition 6. Let Σ be a signature. A Σ-THEORY is any set of Σ-sentences. $\square$

Given a Σ-theory T, a *T-interpretation* is a Σ-interpretation that satisfies all sentences in T. A Σ-formula φ is:

- *T-valid*, if it is satisfied by all T-interpretations;
- *T-satisfiable*, if it is satisfied by some T-interpretation;
- *T-unsatisfiable*, if it is not T-satisfiable.

Given a Σ-theory T, we can define several decision problems for T. More precisely, if L is a set of formulae then

- the *validity problem* of T with respect to L is the problem of deciding, for each formula φ in L, whether or not φ is T-satisfiable;
- the *satisfiability problem* of T with respect to L is the problem of deciding, for each formula φ in L, whether or not φ is T-satisfiable;
- the *unsatisfiability problem* of T with respect to L is the problem of deciding, for each formula φ in L, whether or not φ is T-unsatisfiable.

When we mention a decision problem without specifying the set of formulae L, we implicitly assume that L is the set of all Σ-formulae. For instance, if T is a Σ-theory, the validity problem of T is the problem of deciding, for each Σ-formula φ, whether or not φ is T-satisfiable.

When we prefix the name of a decision problem with "quantifier-free", we implicitly assume that L is the set of all quantifier-free Σ-formulae. For instance, the quantifier-free satisfiability problem of a Σ-theory T is the problem of deciding, for each quantifier-free Σ-formula φ, whether or not φ is T-satisfiable.

Sometimes, it is convenient to reduce the (quantifier-free) validity problem of a theory T to the (quantifier-free) satisfiability problem of T. Note that this is always possible because every formula φ is T-valid if and only if $\neg\varphi$ is T-unsatisfiable. Thus, in order to test φ for T-validity, one only needs to test $\neg\varphi$ for T-unsatisfiability.

Definition 7. A theory is UNIVERSAL if all its sentences are of the form $(\forall *)\varphi$, where φ is quantifier-free. $\square$

In this report, we will use the usual notion of stable infiniteness for a theory, together with its "dual" one, which we call stable finiteness.

Definition 8. A Σ-theory T is STABLY INFINITE (respectively, STABLY FINITE) if every quantifier-free Σ-formula φ is T-satisfiable if and only if it is satisfied by a T-interpretation $\mathcal{A}$ whose domain A is infinite (respectively, finite). $\square$

Examples of stably infinite theories include the theory of equality,[3] the theory of integers, the theory of rationals, the theory of lists, and the theory of arrays, and the theory of sets.

Examples of stably finite theories include the theory of equality, all theories satisfied only by finite interpretations, and all theories axiomatized by formulae in the Bernays-Schönfinkel-Ramsey class.

Note that a theory can be both stably finite and stably infinite, an example given by the theory of equality.

Definition 9. A Σ-theory T is CONVEX if for every conjunction Γ of Σ-literals and for every disjunction $\bigvee_{i=1}^{n} x_i = y_i$,

$$T \cup \Gamma \models \bigvee_{i=1}^{n} x_i = y_i \qquad \text{iff} \qquad T \cup \Gamma \models x_j = y_j, \text{for some } j \in \{1, \ldots, n\}. \qquad \square$$

Examples of convex theories include the theory of equality, the theory of rationals, and the theory of lists.

3 Nelson-Oppen

Let Σ_1 and Σ_2 be signatures, and let T_i be a Σ_i-theory, for $i = 1, 2$. Assume that there exist decision procedures P_1 and P_2 such that, for $i = 1, 2$, P_i can decide the quantifier-free satisfiability problem of T_i. The Nelson-Oppen combination method uses P_1 and P_2 as black boxes in order to decide the $(T_1 \cup T_2)$-satisfiability of quantifier-free $(\Sigma_1 \cup \Sigma_2)$-formulae.

Provided that $\Sigma_1 \cap \Sigma_2 = \emptyset$, and that T_1 and T_2 are stably infinite, the Nelson-Oppen combination method provides a decision procedure for the quantifier-free satisfiability problem of $T_1 \cup T_2$.

We now describe the Nelson-Oppen combination method. Without loss of generality, we restrict ourselves to conjunctions of literals. Note that this can always be done because every quantifier-free formula φ can be effectively converted into an equisatisfiable formula in disjunctive normal form $\psi_1 \vee \cdots \vee \psi_n$, where each ψ_i is a conjunction of literals. Then φ is satisfiable if and only if at least one of the disjuncts ψ_i is satisfiable.

Thus, let Γ be a conjunction of $(\Sigma_1 \cup \Sigma_2)$-literals. The Nelson-Oppen method consists of two phases: *variable abstraction* and *check*.

In the variable abstraction phase we convert Γ into a conjunction $\Gamma_1 \cup \Gamma_2$ satisfying the following properties:

(a) each literal in Γ_i is a Σ_i-literal, for $i = 1, 2$;

(b) $\Gamma_1 \cup \Gamma_2$ is $(T_1 \cup T_2)$-satisfiable if and only if so is Γ.

[3]Since we regard $=$ as a logical symbol, for us the theory of equality and the empty theory are the same theory.

Note that all properties can be effectively enforced with the help of new auxiliary variables.

We call $\Gamma_1 \cup \Gamma_2$ a conjunction of literals in *separate* form. Moreover, we denote with $\mathit{shared}(\Gamma_1, \Gamma_2)$ the set of variables occurring in both Γ_1 and Γ_2, that is, $\mathit{shared}(\Gamma_1, \Gamma_2) = \mathit{vars}(\Gamma_1) \cap \mathit{vars}(\Gamma_2)$.

In order to describe the check phase, we introduce the notion of *arrangement*.

Definition 10. Let E be an equivalence relation over some set V of variables. The *arrangement* of V induced by E is defined as the conjunction:

$$\begin{aligned} \mathit{arr}(V, E) = \{x = y \mid x, y \in V \text{ and } (x, y) \in E\} \cup \\ \{x \neq y \mid x, y \in V \text{ and } (x, y) \notin E\} \,. \end{aligned}$$

□

Let $\Gamma_1 \cup \Gamma_2$ be a conjunction of literals in separate form, and let $V = \mathit{shared}(\Gamma_1, \Gamma_2)$. In the check phase we perform the following two steps, for each equivalence relation E of V:

Step 1. If $\Gamma_1 \cup \mathit{arr}(V, E)$ is T_1-satisfiable go to the next step; otherwise output `fail`;

Step 2. If $\Gamma_2 \cup \mathit{arr}(V, E)$ is T_2-satisfiable output `succeed`; otherwise output `fail`.

If there exists an equivalence relation E of V for which we output `succeed` then we declare that $\Gamma_1 \cup \Gamma_2$ is $(T_1 \cup T_2)$-satisfiable. If instead we output `fail` for each equivalence relation E of V then we declare that $\Gamma_1 \cup \Gamma_2$ is $(T_1 \cup T_2)$-unsatisfiable.

Provided that the signatures Σ_1 and Σ_2 are disjoint, and that the theories T_1 and T_2 are stably infinite, then the Nelson-Oppen method just described is correct. The following theorem summarizes this result.

Theorem 11. *Let T_i be a stably infinite Σ_i-theory, for $i = 1, 2$, and let $\Sigma_1 \cap \Sigma_2 = \emptyset$. Also, assume that the quantifier-free T_i-satisfiability problem is decidable. Then the Nelson-Oppen combination method provides a decision procedure for the quantifier-free satisfiability problem of $T_1 \cup T_2$.* □

3.1 An example in which all goes well

Let $T_{\mathbb{R}}$ be the theory of reals, let $\Sigma_f = \{f\}$, where f is a unary function symbol, and let T_f be the theory of equality over the signature Σ_f.

Since $\Sigma_{\mathbb{R}} \cap \Sigma_f = \emptyset$, and since both $T_{\mathbb{R}}$ and T_f are stably infinite, Theorem 11 tells us that the Nelson-Oppen method is able to correctly combine $T_{\mathbb{R}}$ and T_f.

Consider the conjunction

$$\Gamma = \left\{ \begin{array}{l} x + y = z \,, \\ f(x) \neq f(y) \end{array} \right\} .$$

We have that Γ is $(T_{\mathbb{R}} \cup T_f)$-satisfiable: A $(T_{\mathbb{R}} \cup T_f)$-interpretation $\mathcal{A}$ satisfying Γ can be obtained by letting $A = \mathbb{R}$, $x^{\mathcal{A}} = 1$, $y^{\mathcal{A}} = 2$, $z^{\mathcal{A}} = 3$, and $f^{\mathcal{A}}(a) = a$, for each $a \in \mathbb{R}$.

Let us apply the Nelson-Oppen combination method to Γ. In the variable abstraction phase we do not need to introduce new variables, and we simply return the conjunctions

$$\Gamma_{\mathbb{R}} = \{x + y = z\}\,, \qquad\qquad \Gamma_f = \{f(x) \neq f(y)\}\,.$$

Since $\mathit{shared}(\Gamma_{\mathbb{R}}, \Gamma_f) = \{x, y\}$, there are only two equivalence relations to examine: either $(x, y) \in E$ or $(x, y) \notin E$. In the former case $\Gamma_f \cup \{x = y\}$ is T_f-unsatisfiable. However, in the latter case we have that $\Gamma_{\mathbb{R}} \cup \{x \neq y\}$ is $T_{\mathbb{R}}$-satisfiable and that $\Gamma_f \cup \{x \neq y\}$ is T_f-satisfiable. Thus, we correctly conclude that Γ is $(T_{\mathbb{R}} \cup T_f)$-satisfiable.

3.2 An example in which something goes wrong

Let $T_{\mathbb{R}}$ be the theory of reals, let $\Sigma_{\mathbb{M}} = \{f, <\}$, and let $T_{\mathbb{M}}$ be the theory defined by

$$T_{\mathbb{M}} = \left\{ \begin{array}{l} (\forall x)\neg(x < x)\,, \\ (\forall x)(\forall y)(\forall z)[x < y \ \wedge \ y < z \ \rightarrow \ x < z]\,, \\ (\forall x)(\forall y)[x < y \rightarrow f(x) < f(y)] \end{array} \right\}\,,$$

Intuitively, $T_{\mathbb{M}}$ models f as a monotone increasing function with respect to the order $<$.

Since $\Sigma_{\mathbb{R}} \cap \Sigma_{\mathbb{M}} = \{<\}$, the Nelson-Oppen combination method cannot be applied in order to combine $T_{\mathbb{R}}$ and $T_{\mathbb{M}}$. As an example of what can go wrong, consider the conjunction

$$\Gamma = \left\{ \begin{array}{c} u < v\,, \\ u = x + 1\,, \\ v = y + 1\,, \\ \neg(f(x) < f(y)) \end{array} \right\}\,.$$

We have that Γ is $(T_{\mathbb{R}} \cup T_{\mathbb{M}})$-unsatisfiable. In particular, the unsatisfiability is caused by the shared predicate symbol $<$. In fact, the first three literals imply $x < y$, whereas the last literal implies $\neg(x < y)$.

However, the Nelson-Oppen method is unable to detect the unsatisfiability. To see this, let us apply the method to Γ. In the variable abstraction phase, we obtain the conjunctions

$$\Gamma_{\mathbb{R}} = \left\{ \begin{array}{l} u < v\,, \\ u = x + 1\,, \\ v = y + 1 \end{array} \right\}\,, \qquad\qquad \Gamma_{\mathbb{M}} = \left\{ \begin{array}{l} u < v\,, \\ \neg(f(x) < f(y)) \end{array} \right\}\,.$$

Let $V = \mathit{shared}(\Gamma_{\mathbb{R}}, \Gamma_{\mathbb{M}}) = \{x, y, u, v\}$. For the check phase, consider the equivalence relation E induced by the partition $\{\{x\}, \{y\}, \{u\}, \{v\}\}$. In other words, E models all variables in V as different. We have that both $\Gamma_{\mathbb{R}} \cup \mathit{arr}(V, E)$ is $T_{\mathbb{R}}$-satisfiable and that $\Gamma_{\mathbb{M}} \cup \mathit{arr}(V, E)$ is $T_{\mathbb{M}}$-satisfiable. Thus, the Nelson-Oppen method *incorrectly* concludes that Γ is $(T_{\mathbb{R}} \cup T_{\mathbb{M}})$-satisfiable.

The Nelson-Oppen combination method is unable to detect the unsatisfiability because it does not take into account the shared predicate symbol $<$. We will see in the next section that we can detect the unsatisfiability by using C-tableaux.

Abstraction rule

$$\frac{}{t = w}$$

Where t is either a Σ_1-term or a Σ_2-term, and w is a newly generated variable.

Decomposition rules

$$\frac{}{x = y \mid x \neq y} \qquad\qquad \frac{}{P(x_1, \ldots, x_n) \mid \neg P(x_1, \ldots, x_n)}$$

Where $x, y, x_1, \ldots, x_n$ are variables already occurring in the branch and $P \in \Sigma_1^{\mathrm{P}} \cap \Sigma_2^{\mathrm{P}}$.

Closure rule

$$\frac{\begin{array}{c}\ell_1\\ \vdots\\ \ell_n\end{array}}{\mathit{false}}$$

Provided that there exists an index $i \in \{1, 2\}$ such that $\ell_1, \ldots, \ell_n$ are Σ_i-literals and $\{\ell_1, \ldots, \ell_n\}$ is T_i-unsatisfiable.

Figure 1: C-tableau rules.

4 C-tableaux

Let Σ_1 and Σ_2 be arbitrary signatures (that is, not necessarily disjoint), and let T_i be a universal Σ_i-theory, for $i = 1, 2$. Also, assume that there exist decision procedures P_1 and P_2 such that, for $i = 1, 2$, P_i can decide the quantifier-free satisfiability problem of T_i. Using P_1 and P_2 as black boxes, C-tableaux provide a method for checking the $(T_1 \cup T_2)$-satisfiability of quantifier-free $(\Sigma_1 \cup \Sigma_2)$-formulae.

We now describe C-tableaux. As usual, we restrict ourselves to conjunctions of $(\Sigma_1 \cup \Sigma_2)$-literals. Moreover, by using the variable abstraction phase of the the Nelson-Oppen combination method, we can further restrict ourselves to conjunction of literals in separate form.

Definition 12 (C-tableaux). Let $\Gamma = \Gamma_1 \cup \Gamma_2$ be a conjunction of literals in separate form. An INITIAL C-TABLEAU for Γ is a tree consisting of one branch whose nodes are labeled with the literals in Γ. A C-TABLEAU for Γ is either an initial C-tableau for Γ or is obtained by applying the rules in Figure 1 to an initial C-tableau for Γ. $\square$

The intuition behind the rules in Figure 1 is as follows. The *closure rule* is used in order to detect inconsistencies. The *decomposition rule* is used to let the decision procedures for T_1 and T_2 "agree" on the truth-value of every atom.

The intuition behind the *abstraction rule* is more complex. Suppose that t is a Σ_1-term but not a Σ_2-term. Then the decision procedure for T_1 "knows" about t, but the decision procedure for T_2 does not. After an application of the abstraction rule, the decision procedure for T_2 is aware of the existence of

We now define when a C-tableau is closed.

Definition 13. Let B be a branch of a C-tableau T. We say that B is CLOSED if it contains the literal *false*. A branch which is not closed is OPEN. A C-tableau is CLOSED if so are all its branches; otherwise it is OPEN. □

In Section 6 we will prove that C-tableaux are sound and complete for quantifier-free *unsatisfiability* problem of $(T_1 \cup T_2)$. More specifically, for any conjunction $\Gamma = \Gamma_1 \cup \Gamma_2$ in separate form, we have:

- **Soundness.** If there exists a closed C-tableau for Γ then Γ is $(T_1 \cup T_2)$-unsatisfiable;
- **Completeness.** If Γ is $(T_1 \cup T_2)$-unsatisfiable then Γ has a closed C-tableau.

In general, C-tableaux are not terminating. Nontermination is caused by the abstraction rule, which requires that we add a literal of the form $t = w$, for each $(\Sigma_1 \cup \Sigma_2)$-term t. Unfortunately, when $\Sigma_1^{\mathrm{F}} \cup \Sigma_2^{\mathrm{F}} \neq \emptyset$, there is an infinite number of such terms.[4]

Although in general C-tableaux are not terminating, they can form the basis for decidability results. We will address the issue of decidability in Sections 10–10.

4.1 An example

Let $T_{\mathbb{R}}$ be the theory of reals, let $\Sigma_{\mathbb{M}} = \{f, <\}$, and let $T_{\mathbb{M}}$ be the theory defined by

$$T_{\mathbb{M}} = \left\{ \begin{array}{l} (\forall x)\neg(x < x)\,, \\ (\forall x)(\forall y)(\forall z)[x < y \ \wedge \ y < z \ \rightarrow \ x < z]\,, \\ (\forall x)(\forall y)[x < y \rightarrow f(x) < f(y)] \end{array} \right\}.$$

In Subsection 3.2 we saw that the Nelson-Oppen combination method cannot be used in order to combine $T_{\mathbb{R}}$ and $T_{\mathbb{M}}$. In particular, we saw that the Nelson-Oppen combination method *incorrectly* concludes that the conjunction

$$\Gamma = \left\{ \begin{array}{c} u < v\,, \\ u = x + 1\,, \\ v = y + 1\,, \\ \neg(f(x) < f(y)) \end{array} \right\}$$

is $(T_{\mathbb{R}} \cup T_{\mathbb{M}})$-satisfiable, despite the fact that Γ is $(T_{\mathbb{R}} \cup T_{\mathbb{M}})$-unsatisfiable.

Let us see what happens if, instead of the Nelson-Oppen combination method, we use C-tableaux. Figure 2 shows a closed C-tableau for Γ. Denoting with ℓ_i the literal labeling

[4]Technically speaking, nontermination is due to more than the presence of infinitely many terms. The problem is that, in general, the abstraction rule cannot be safely restricted to a finite subset of $(\Sigma_1 \cup \Sigma_2)$-terms without sacrificing completeness.

$$
\begin{array}{ll}
1. & u < v \\
2. & u = x + 1 \\
3. & v = y + 1 \\
4. & \neg(f(x) < f(y))
\end{array}
$$

$$
\begin{array}{llcll}
5. & x < y & \qquad & 7. & \neg(x < y) \\
6. & \mathit{false} & & 8. & \mathit{false}
\end{array}
$$

Figure 2: A closed C-tableau.

node i, the inferences can be justified as follows:

- $\ell_1, \ell_2, \ell_3, \ell_4$ are the formulae occurring in Γ.
- ℓ_5 and ℓ_7 are obtained by means of an application of the second decomposition rule.
- ℓ_6 is obtained by using the closure rule, exploiting the fact that $\{\ell_4, \ell_5\}$ is $T_{\mathbb{M}}$-unsatisfiable.
- ℓ_8 is obtained by using the closure rule, exploiting the fact that $\{\ell_1, \ell_2, \ell_3, \ell_5\}$ is $T_{\mathbb{R}}$-unsatisfiable.

Since the C-tableau in Figure 2 is closed, we *correctly* conclude that Γ is $(T_{\mathbb{R}} \cup T_{\mathbb{M}})$-unsatisfiable.

5 The combination theorem

In this section we state and prove a fundamental model-theoretic result that forms the basis for the proof of completeness of C-tableaux. Early forms of this result are due independently to Ringeissen [8] and Tinelli and Harandi [12]. A refinement was later made by Tinelli and Ringeissen [13]. The version presented here is due to Zarba [16].

Theorem 14 (Combination Theorem). *Let Σ_1 and Σ_2 be signatures, let Φ_i be a set of Σ_i-formulae, for $i = 1, 2$, and let $V_i = vars(\Phi_i)$.*

Then $\Phi_1 \cup \Phi_2$ is satisfiable if and only if there exists a Σ_1-interpretation $\mathcal{A}$ satisfying Φ_1 and a Σ_2-interpretation $\mathcal{B}$ satisfying Φ_2 such that

$$\mathcal{A}^{\Sigma_1 \cap \Sigma_2, V_1 \cap V_2} \cong \mathcal{B}^{\Sigma_1 \cap \Sigma_2, V_1 \cap V_2} .$$ □

Proof. To make the notation more concise, let $\Sigma = \Sigma_1 \cap \Sigma_2$ and $V = V_1 \cap V_2$.

Next, assume that $\Phi_1 \cup \Phi_2$ is satisfiable, and let $\mathcal{F}$ be an interpretation satisfying $\Phi_1 \cup \Phi_2$. Then, by letting $\mathcal{A} = \mathcal{F}^{\Sigma_1, V_1}$ and $\mathcal{B} = \mathcal{F}^{\Sigma_2, V_2}$, we clearly have that:

- $\mathcal{A}$ satisfies Φ_1;

- $\mathcal{B}$ satisfies Φ_2;
- $\mathcal{A}^{\Sigma,V} \cong \mathcal{B}^{\Sigma,V}$.

Vice versa, assume that there exists an interpretation $\mathcal{A}$ satisfying Φ_1 and an interpretation $\mathcal{B}$ satisfying Φ_2 such that $\mathcal{A}^{\Sigma,V} \cong \mathcal{B}^{\Sigma,V}$, and let $h : A \to B$ be an isomorphism of $\mathcal{A}^{\Sigma,V}$ into $\mathcal{B}^{\Sigma,V}$. We define an interpretation $\mathcal{F}$ by letting $M = A$ and:

- for variables and constant symbols:

$$u^{\mathcal{F}} = \begin{cases} u^{\mathcal{A}}\,, & \text{if } u \in (\Sigma_1^{\mathrm{C}} \cup V_1)\,, \\ h^{-1}(u^{\mathcal{B}})\,, & \text{if } u \in (\Sigma_2^{\mathrm{C}} \cup V_2) \setminus (\Sigma_1^{\mathrm{C}} \cup V_1)\,, \end{cases}$$

- for function symbols of arity n:

$$f^{\mathcal{F}}(a_1, \ldots, a_n) = \begin{cases} f^{\mathcal{A}}(a_1, \ldots, a_n)\,, & \text{if } f \in \Sigma_1^{\mathrm{F}}\,, \\ h^{-1}(f^{\mathcal{B}}(h(a_1), \ldots, h(a_n)))\,, & \text{if } f \in \Sigma_2^{\mathrm{F}} \setminus \Sigma_1^{\mathrm{F}}\,, \end{cases}$$

- for predicate symbols of arity n:

$$\begin{array}{ll} (a_1, \ldots, a_n) \in P^{\mathcal{F}} \iff (a_1, \ldots, a_n) \in P^{\mathcal{A}}\,, & \text{if } P \in \Sigma_1^{\mathrm{P}} \\ (a_1, \ldots, a_n) \in P^{\mathcal{F}} \iff (h(a_1), \ldots, h(a_n)) \in P^{\mathcal{B}}\,, & \text{if } P \in \Sigma_2^{\mathrm{P}} \setminus \Sigma_1^{\mathrm{P}}\,. \end{array}$$

By construction, $\mathcal{F}^{\Sigma_1,V_1} \cong \mathcal{A}$. In addition, it is easy to verify that h is an isomorphism of $\mathcal{F}^{\Sigma_2,V_2}$ into $\mathcal{B}$. Thus, by Proposition 3, $\mathcal{F}$ satisfies $\Phi_1 \cup \Phi_2$. ■

6 Soundness and completeness

In this section we prove that C-tableaux are sound and complete for the $(T_1 \cup T_2)$-unsatisfiability of quantifier-free $(\Sigma_1 \cup \Sigma_2)$-formulae.

In our proofs, we will use the following definitions.

Definition 15. A branch B of a C-tableau T is SATURATED if no application of any rule in Figure 1 can add new formulae to B. □

Definition 16. Let T be a theory. A branch B of a C-tableau T is T-SATISFIABLE if the set of all literals occurring in it is T-satisfiable.

A C-tableau is T-SATISFIABLE if at least one of its branches is satisfiable. □

When doing the completeness proof, the Herbrand Theorem 5 will play a crucial role. Consequently, in order to later said theorem, we make the technical assumption that $Terms(\Sigma_1 \cup \Sigma_2, vars(\Gamma)) \neq \emptyset$, where Γ is the conjunction of literals whose satisfiability is being checked. Note that this assumption is not too restrictive since it is verified whenever $\Sigma_1^{\mathrm{C}} \cup \Sigma_2^{\mathrm{C}} \cup vars(\Gamma) \neq \emptyset$, which is virtually always true in practical applications.

6.1 Soundness

C-tableaux are clearly sound, as the following theorem states.

Theorem 17 (Soundness). *Let $\Gamma = \Gamma_1 \cup \Gamma_2$ be a conjunction of literals in separate form. If there exists a closed C-tableau for Γ, then Γ is $(T_1 \cup T_2)$-unsatisfiable.* □

PROOF. Let T be a closed C-tableau for Γ, and suppose, by contradiction, that Γ is $(T_1 \cup T_2)$-satisfiable. Since the rules in Figure 1 preserve $(T_1 \cup T_2)$-satisfiability of C-tableau, it follows that there exists some branch B of T which is $(T_1 \cup T_2)$-satisfiable. But since T is closed, B must also be closed, which is a contradiction because a closed branch cannot be $(T_1 \cup T_2)$-satisfiable. ■

6.2 Completeness

The completeness proof is more complex, and is based upon the Herbrand Theorem 5 and the Combination Theorem 14.

Proposition 18. *Let B be a (not necessarily finite) open branch of a C-tableau T, and let θ_i be the collection of Σ_i-literals occurring in B, for $i = 1, 2$. Then θ_i is T_i-satisfiable, for $i = 1, 2$.* □

PROOF. Since B is open, every finite subset of θ_1 is T_1-satisfiable. Hence, every finite subset of $T_1 \cup \theta_1$ is satisfiable. By compactness, $T_1 \cup \theta_1$ is satisfiable, implying that θ_1 is T_1-satisfiable. Similarly, one can show that θ_2 is T_2-satisfiable. ■

For the rest of this section, let us fix an open and saturated branch B, and let θ_i be the collection of Σ_i-literals occurring in B, for $i = 1, 2$, and let $V = \mathit{vars}(\mathsf{B})$. Note that every literal in B is either a Σ_1-literal or a Σ_2-literal, and therefore $\mathsf{B} = \theta_1 \cup \theta_2$.

By Proposition 18, there exist a T_1-interpretation $\mathcal{A}$ satisfying θ_1 and a T_2-interpretation $\mathcal{B}$ satisfying θ_2. In addition, since T_1 and T_2 are universal, by Theorem 5 and by saturation with respect to the abstraction rule, we can assume without loss of generality that $A = V^{\mathcal{A}}$ and $B = V^{\mathcal{B}}$. Thus, we can fix a function $\mathit{name}_{\mathcal{A}} : A \to V$ such that

$$[\mathit{name}_{\mathcal{A}}(a)]^{\mathcal{A}} = a\,, \qquad\qquad \text{for each } a \in A\,.$$

The next step of the completeness proof is to merge the structures $\mathcal{A}$ and $\mathcal{B}$ into a single structure $\mathcal{F}$ satisfying $T_1 \cup T_2 \cup \theta_1 \cup \theta_2$. Clearly, this goal can be accomplished by an application of the Combination Theorem 14 if we can show that $\mathcal{A}^{(\Sigma_1 \cap \Sigma_2) \cup V}$ and $\mathcal{B}^{(\Sigma_1 \cap \Sigma_2) \cup V}$ are isomorphic. Accordingly, we define a function $h : A \to B$ by letting

$$h(a) = [\mathit{name}_{\mathcal{A}}(a)]^{\mathcal{B}}\,, \qquad\qquad \text{for each } a \in A\,.$$

The following five propositions show that h is an isomorphism of $\mathcal{A}^{(\Sigma_1 \cap \Sigma_2) \cup V}$ into $\mathcal{B}^{(\Sigma_1 \cap \Sigma_2) \cup V}$.

Proposition 19. *$x^{\mathcal{A}} = y^{\mathcal{A}}$ if and only if $x^{\mathcal{B}} = y^{\mathcal{B}}$, for every $x, y \in V$.* □

PROOF. By saturation with respect to the first decomposition rule. ■

Proposition 20. *$h(x^{\mathcal{A}}) = x^{\mathcal{B}}$, for every $x \in V$.* □

PROOF. Let $x^{\mathcal{A}} = a$ and let $name_{\mathcal{A}}(a) = y$. Then $x^{\mathcal{A}} = y^{\mathcal{A}}$, which implies $x^{\mathcal{B}} = y^{\mathcal{B}}$ by Proposition 19. Thus $h(x^{\mathcal{A}}) = h(a) = [name_{\mathcal{A}}(a)]^{\mathcal{B}} = y^{\mathcal{B}} = x^{\mathcal{B}}$. ■

Proposition 21. *h is injective.* □

PROOF. Let $h(a_1) = h(a_2)$. Then, by letting $name_{\mathcal{A}}(a_i) = x_i$, for $i = 1, 2$, it follows that $x_1^{\mathcal{B}} = x_2^{\mathcal{B}}$. By Proposition 19, $x_1^{\mathcal{A}} = x_2^{\mathcal{A}}$, which in turn implies $a_1 = a_2$. ■

Proposition 22. *h is surjective.* □

PROOF. Let $b \in B$. Then there exists a variable $x \in V$ such that $x^{\mathcal{B}} = b$. By Proposition 20, $h(x^{\mathcal{A}}) = x^{\mathcal{B}} = b$, and therefore h is surjective. ■

Proposition 23. *h is a quasi-embedding of $\mathcal{A}^{(\Sigma_1 \cap \Sigma_2) \cup V}$ into $\mathcal{B}^{(\Sigma_1 \cap \Sigma_2) \cup V}$.* □

PROOF. Proposition 20 implies that $h(x^{\mathcal{A}}) = x^{\mathcal{B}}$, for each $x \in V$. On the other hand, if $c \in \Sigma_1^{\mathrm{C}} \cap \Sigma_2^{\mathrm{C}}$, then by saturation with respect to the abstraction rule a literal of the form $c = x$ must occur in B, and therefore $h(c^{\mathcal{A}}) = h(x^{\mathcal{A}}) = x^{\mathcal{B}} = c^{\mathcal{B}}$.

Next, let $f \in \Sigma_1^{\mathrm{F}} \cap \Sigma_2^{\mathrm{F}}$, and let $a = f^{\mathcal{A}}(a_1, \ldots, a_n)$, where $a_1, \ldots, a_n \in A$. Then there exist variables $x_1, \ldots, x_n \in V$ such that $a_i = x_i^{\mathcal{A}}$, for each $i = 1, \ldots, n$. By Proposition 20 we have that $h(a_i) = x_i^{\mathcal{B}}$, for each $i = 1, \ldots, n$. Note also that $[f(x_1, \ldots, x_n)]^{\mathcal{A}} = [name_{\mathcal{A}}(a)]^{\mathcal{A}}$, which by Proposition 19 yields $[f(x_1, \ldots, x_n)]^{\mathcal{B}} = [name_{\mathcal{A}}(a)]^{\mathcal{B}}$. Thus, we obtain $h(f^{\mathcal{A}}(a_1, \ldots, a_n)) = h(a) = [name_{\mathcal{A}}(a)]^{\mathcal{B}} = [f(x_1, \ldots, x_n)]^{\mathcal{B}} = f^{\mathcal{B}}(x_1^{\mathcal{B}}, \ldots, x_n^{\mathcal{B}}) = f^{\mathcal{B}}(h(a_1), \ldots, h(a_n))$.

Next, assume that $(a_1, \ldots, a_n) \in P^{\mathcal{A}}$, where $P \in \Sigma_1^{\mathrm{P}} \cap \Sigma_2^{\mathrm{P}}$ and $a_i \in A$, for $i = 1, \ldots, n$. Then there exist variables $x_1, \ldots, x_n \in V$ such that $a_i = x_i^{\mathcal{A}}$, for each $i = 1, \ldots, n$. By Proposition 20 we have $h(a_i) = x_i^{\mathcal{B}}$, for each $i = 1, \ldots, n$. By saturation with respect to the second decomposition rule, $P(x_1, \ldots, x_n)$ is in B, so that $(x_1^{\mathcal{B}}, \ldots, x_n^{\mathcal{B}}) \in P^{\mathcal{B}}$. But this implies $(h(a_1), \ldots, h(a_n)) \in P^{\mathcal{B}}$.

Analogously one can prove that if $(h(a_1), \ldots, h(a_n)) \in P^{\mathcal{B}}$ then $(a_1, \ldots, a_n) \in P^{\mathcal{A}}$. ■

We are now able to apply the Combination Theorem 14 and obtain the existence of a $(T_1 \cup T_2)$-interpretation $\mathcal{F}$ satisfying B.

Proposition 24. *Let B be an open and saturated branch of a C-tableau T. Then B is $(T_1 \cup T_2)$-satisfiable.* □

PROOF. Let θ_i be the collection of Σ_i-literals in B, for $i = 1, 2$. By Proposition 18, there exist a T_1-interpretation $\mathcal{A}$ satisfying θ_1 and a T_2-interpretation $\mathcal{B}$ satisfying θ_2. After letting $h(a) = [name_{\mathcal{A}}(a)]^{\mathcal{B}}$, for every $a \in \mathcal{A}$, Proposition 21, 22, and 23 imply that h is an isomorphism of $\mathcal{A}^{(\Sigma_1 \cap \Sigma_2) \cup V}$ into $\mathcal{B}^{(\Sigma_1 \cap \Sigma_2) \cup V}$. Thus, we can apply the the Combination Theorem 14, obtaining the existence of a $(T_1 \cup T_2)$-interpretation $\mathcal{F}$ satisfying $\theta_1 \cup \theta_2$.

Since $\mathsf{B} = \theta_1 \cup \theta_2$, if follows that $\mathcal{F}$ is a $(T_1 \cup T_2)$-interpretation $\mathcal{F}$ satisfying B. ■

We now have everything we need to finish the proof of completeness of C-tableaux.

Theorem 25 (Completeness). *Let $\Gamma = \Gamma_1 \cup \Gamma_2$ be a set of literals in separate form. If Γ is $(T_1 \cup T_2)$-unsatisfiable, then Γ has a closed C-tableau.* □

PROOF. Assume, by contradiction, that Γ has no closed C-tableau, and let T be the initial C-tableau for Γ. Using a fair strategy, apply to T the rules in Figure 1 in all possible ways, obtaining a tableau limit T^∞. Note that, since Γ has no closed C-tableau, T^∞ must contain an open and saturated branch B. By Proposition 24, B is $(T_1 \cup T_2)$-satisfiable, which implies that also Γ is $(T_1 \cup T_2)$-satisfiable, a contradiction. ■

7 The quest for efficiency

C-tableaux are essentially a *ground total multi-theory reasoning* calculus where the *foreground reasoner* decides what tableau rules to apply, and the two *background reasoners*—the decision procedures for T_1 and T_2—are in charge of detecting branch closure. The cooperation of the two background reasoners is done with the decomposition rules. The decomposition rules are, however, inherently nondeterministic, and a blind search performed by the foreground reasoner is unlikely to find the applications of the decomposition rules that lead to the shorter proofs.

The problem is that the foreground reasoner has no knowledge of the features of the theories to combine. The background reasoners, with their better domain-specific knowledge, are more qualified to direct the search toward the "best" applications of the decomposition rules. Our goal is therefore to devise a mechanism to make the background reasoners help the foreground reasoner make the tableau construction more efficient and less nondeterministic.

Following an idea of Tinelli [11], this can be done in a *partial multi-theory reasoning* setting, by allowing the background reasoners to return *residues*. More precisely, we define a residue version of C-tableaux by replacing the decomposition rules with the residue rule shown in Figure 3

The residue rule in Figure 3 helps making the exploration of the search space more efficient. In addition, the rule effectively reduces the search space in the presence of convex theories. In fact, while in general residues are disjunctions of atoms, when T_i is convex the residues returned by the background reasoner for T_i are restricted to atoms.

Residue rule

$$\frac{\begin{matrix}\varphi_1\\ \vdots\\ \varphi_h\end{matrix}}{\psi_1 \;|\; \ldots \;|\; \psi_k}$$

Provided there is an index $i \in \{1,2\}$ such that:

- if T_i is convex, then $k = 1$;
- $\varphi_1, \ldots, \varphi_h$ are Σ_i-literals;
- for each $j = 1, \ldots, k$, ψ_j is either of the form $x = y$ or of the form $P(x_1, \ldots, x_n)$, where $x, y, x_1, \ldots, x_n$ are variables already occurring in the branch, and $P \in \Sigma_1^{\mathrm{P}} \cap \Sigma_2^{\mathrm{P}}$;
- $T_i \cup \{\varphi_1, \ldots, \varphi_h\} \models \psi_1 \vee \cdots \vee \psi_k$.

Figure 3: The residue rule.

7.1 An example

Let $T_{\mathbb{R}}$ be the theory of reals, let $\Sigma_{\mathbb{M}} = \{f, <\}$, and let $T_{\mathbb{M}}$ be the theory defined by

$$T_{\mathbb{M}} = \left\{ \begin{array}{l} (\forall x)\neg(x < x)\,, \\ (\forall x)(\forall y)(\forall z)[x < y \;\wedge\; y < z \;\rightarrow\; x < z]\,, \\ (\forall x)(\forall y)[x < y \rightarrow f(x) < f(y)] \end{array} \right\}.$$

In Subsection 4.1 we used the version of C-tableaux without the residue rule to show that the conjunction

$$\Gamma = \left\{ \begin{array}{c} u < v\,, \\ u = x + 1\,, \\ v = y + 1\,, \\ \neg(f(x) < f(y)) \end{array} \right\}$$

is $(T_{\mathbb{R}} \cup T_{\mathbb{M}})$-unsatisfiable.

Let us now detect the unsatisfiability using the residue rule. Figure 4 shows a closed C-tableau with residues that proves that Γ is $(T_{\mathbb{R}} \cup T_{\mathbb{M}})$-unsatisfiable.

Denoting with ℓ_i the literal labeling node i, the inferences can be justified as follows:

- $\ell_1, \ell_2, \ell_3, \ell_4$ are the formulae occurring in Γ.
- ℓ_5 is obtained by means of an application of the residue rule since $T_{\mathbb{R}} \cup \{\ell_1, \ell_2, \ell_3\} \models \ell_5$.
- ℓ_6 is obtained by using the contradiction rule, exploiting the fact that $\{\ell_4, \ell_5\}$ is $T_{\mathbb{M}}$-unsatisfiable.

1.	$u < v$
2.	$u = x + 1$
3.	$v = y + 1$
4.	$\neg(f(x) < f(y))$
5.	$x < y$
6.	*false*

Figure 4: A closed C-tableau with residues.

7.2 Soundness and completeness

Soundness of the residue version of C-tableaux immediately follows by inspection of the residue rule, whereas completeness is a consequence of the following proposition.

Proposition 26. *Let* B *be an open branch, and assume that no application of any abstraction, closure, and residue rule can add new formulae to* B*. Then* B *is* $(T_1 \cup T_2)$*-satisfiable.* □

PROOF. Consider the set

$$\mathsf{B}' = \mathsf{B} \cup \{\neg\psi : \psi \text{ is an atom and } \psi \notin \mathsf{B}\}\,.$$

Clearly, B' is saturated (with respect to Definition 15). Therefore, if we show that B' is open, by Proposition 24 we obtain that B is $(T_1 \cup T_2)$-satisfiable.

Thus, assume by contradiction that B' is closed. Then there exists an index $i \in \{1, 2\}$ and a finite set θ_i of Σ_i-literals such that $\theta_i \subseteq \mathsf{B}'$ and θ_i is T_i-unsatisfiable. Without loss of generality, let $\theta_i = \{\varphi_1, \ldots, \varphi_h, \neg\psi_1, \ldots, \neg\psi_k\}$, where $\varphi_1, \ldots, \varphi_h$ occur in B and $\psi_1, \ldots, \psi_k$ are atoms not occurring in B. Note that, since B is open, we must have $k > 0$. Moreover, $T_i \cup \{\varphi_1, \ldots, \varphi_h\} \models \psi_1 \vee \cdots \vee \psi_k$. In addition, if T_i is convex, then $T_i \cup \{\varphi_1, \ldots, \varphi_h\} \models \psi_j$, for some $j \in \{1, \ldots, k\}$. But then, by saturation with respect to the residue rule, it follows that $\{\psi_1, \ldots, \psi_k\} \cap \mathsf{B} \neq \emptyset$, a contradiction. ■

8 Stably infinite theories sharing constants

In this section we show that C-tableaux provide a decidability result when combining stably infinite theories whose signatures share up to a finite number of constant symbols. This result was also independently proven in [13].

Let Σ_1 and Σ_2 be signatures, and let T_i be a stably infinite Σ_i-theory, for $i = 1, 2$. Assume that $\Sigma_1 \cap \Sigma_2$ is a finite set of constant symbols. In this case, C-tableaux can be made terminating without sacrificing completeness if we employ the following restrictions.

> **Restriction R1.** All rule applications must be *regular*, that is, an application of a rule R to a branch B is forbidden if it would add a literal already occurring in B.

Restriction R2. A literal $t = w$ can be added to a branch B by means of an application of the abstraction rule only if t is a constant in $\Sigma_1^{\mathrm{C}} \cap \Sigma_2^{\mathrm{C}}$.

We now prove that, by using the restrictions R1 and R2, C-tableaux are terminating, sound, and complete, thus obtaining a decidability result when combining stably infinite theories whose signatures share up to a finite number of constant symbols.

Proposition 27 (Termination). *Using Restrictions R1 and R2, C-tableaux are terminating.* □

PROOF. Let $\Gamma = \Gamma_1 \cup \Gamma_2$ be a conjunction of literals in separate form, and let T be a C-tableau obtained by exhaustively applying, subject to restrictions R1 and R2, the rules in Figure 1 to an initial C-tableau for Γ. We want to show that T is finite.

Because of restriction R2 and the fact that $\Sigma_1^{\mathrm{C}} \cap \Sigma_2^{\mathrm{C}}$ is finite, the abstraction rule can be applied only a finite number of times. Thus, the number of variables introduced by the abstraction rule is finite, which implies that the number of variables occurring in T must also be finite. Because of the regularity restriction R1, it follows that every rule can be applied only a finite number of times, which implies that all branches in T are finite. Thus, T must be finite. ■

Since C-tableaux are already sound without Restrictions R1 and R2, they are also sound with the restrictions.

Proposition 28 (Soundness). *Let $\Gamma = \Gamma_1 \cup \Gamma_2$ be a conjunction of $(\Sigma_1 \cup \Sigma_2)$-literals. Assume that there exists a closed C-tableau for Γ constructed using the rules in Figure 1 and the restrictions R1 and R2. Then Γ is $(T_1 \cup T_2)$-unsatisfiable.* □

Proposition 29. *Let B be an open branch of a C-tableau T. Assume that B is saturated with respect to the rules in Figure 1 and the restrictions R1 and R2. Then B is $(T_1 \cup T_2)$-satisfiable.* □

PROOF. Let $V = vars(\mathsf{B})$, and let θ_i be the set of Σ_i-literals occurring in B, for $i = 1, 2$. Note that $\mathsf{B} = \theta_1 \cup \theta_2$. Since B is open, there exist a T_1-interpretation $\mathcal{A}$ satisfying θ_1 and a T_2-interpretation $\mathcal{B}$ satisfying θ_2.

Because T_1 and T_2 are stably infinite, we can assume without loss of generality that both A and B are enumerable, that is $|A| = |B| = \aleph_0$.

Our goal is to merge the interpretations $\mathcal{A}$ and $\mathcal{B}$ into a $(T_1 \cup T_2)$-interpretation $\mathcal{F}$ satisfying $\theta_1 \cup \theta_2$. This goal can be accomplished by an application of the Combination Theorem 14 if we can show that $\mathcal{A}^{\Sigma_1 \cap \Sigma_2, V} \cong \mathcal{B}^{\Sigma_1 \cap \Sigma_2, V}$.

Let us define a map $f : V^{\mathcal{A}} \to V^{\mathcal{B}}$ by letting

$$f(x^{\mathcal{A}}) = x^{\mathcal{B}}\,, \qquad \text{for each } x \in V\,.$$

By saturation with respect to the first decomposition rule, f is bijective. Thus, $|V^{\mathcal{A}}| = |V^{\mathcal{B}}|$. Since $|A| = |B|$, we also have $|A \setminus V^{\mathcal{A}}| = |B \setminus V^{\mathcal{B}}|$. We can therefore extend f to a bijective function $h : A \to B$.

We claim that h is an isomorphism of $\mathcal{A}^{\Sigma_1 \cap \Sigma_2, V}$ into $\mathcal{B}^{\Sigma_1 \cap \Sigma_2, V}$. To support our claim, we only need to show that $h(c^{\mathcal{A}}) = c^{\mathcal{B}}$, for each constant symbol in $\Sigma_1^{\mathrm{C}} \cap \Sigma_2^{\mathrm{C}}$.

Thus, let c be a constant symbol in $\Sigma_1^{\mathrm{C}} \cap \Sigma_2^{\mathrm{C}}$. By saturation with respect to the abstraction rule, a literal of the form $c = w$ is in B, for some variable w. It follows that $c^{\mathcal{A}} = w^{\mathcal{A}}$ and $c^{\mathcal{B}} = w^{\mathcal{B}}$. Thus $h(c^{\mathcal{A}}) = h(w^{\mathcal{A}}) = w^{\mathcal{B}} = c^{\mathcal{B}}$. ■

Proposition 30 (Completeness). *Let $\Gamma = \Gamma_1 \cup \Gamma_2$ be a conjunction of literals in separate form. If Γ is $(T_1 \cup T_2)$-unsatisfiable then there exists a closed C-tableaux T for Γ constructed using the rules in Figure 1 and the restrictions R1 and R2.* □

PROOF. Assume that Γ is $(T_1 \cup T_2)$-unsatisfiable, and let T be a C-tableau obtained by exhaustively applying, subject to the restrictions R1 and R2, the rules in Figure 1 to an initial C-tableau for Γ.

If T were not closed, then T must contain an open branch that is saturated with respect to the rules in Figure 1 and the restrictions R1 and R2. By Proposition 29, B is $(T_1 \cup T_2)$-satisfiable, which implies that Γ is also $(T_1 \cup T_2)$-satisfiable, a contradiction. ■

Combining Propositions 27, 28, and 30, we obtain the following decidability result.

Theorem 31 (Decidability). *Let Σ_1 and Σ_2 be signatures, and let T_i be a stably infinite Σ_i-theory, for $i = 1, 2$. Assume that $\Sigma_1 \cap \Sigma_2$ is a finite set of constant symbols. Also, assume that the quantifier-free satisfiability problem of T_i is decidable, for $i = 1, 2$.*

Then the quantifier-free satisfiability problem of $T_1 \cup T_2$ is decidable. □

We conclude this section by proving the following complexity result.

Theorem 32 (Complexity). *Let Σ_1 and Σ_2 be signatures, and let T_i be a stably infinite Σ_i-theory, for $i = 1, 2$. Assume that $\Sigma_1 \cap \Sigma_2$ is a finite set of constant symbols. Also, assume that the quantifier-free satisfiability problem of T_i is in $\mathcal{NP}$, for $i = 1, 2$.*

Then the quantifier-free satisfiability problem of $T_1 \cup T_2$ is $\mathcal{NP}$-complete. □

PROOF. $\mathcal{NP}$-hardness follows by the $\mathcal{NP}$-hardness of the propositional calculus.

To show membership in $\mathcal{NP}$, note that we can check that a $(\Sigma_1 \cup \Sigma_2)$-formula φ is $(T_1 \cup T_2)$-satisfiable by:

1. guessing a disjunct Γ of a disjunctive normal form of φ;
2. converting Γ into a $(T_1 \cup T_2)$-equisatisfiable conjunction $\Gamma' = \Gamma_1 \cup \Gamma_2$ in separate form;
3. guessing a branch B of a C-tableau for Γ';
4. verifying that B is open and saturated.

Since the size of Γ' is polynomially bounded by the size of φ, to prove $\mathcal{NP}$-completeness we only need to show that the size of B is polynomially bounded by the size of Γ'.

Let n be the number of variables occurring in Γ', and let $k = |\Sigma_1^{\mathrm{C}} \cap \Sigma_2^{\mathrm{C}}|$. Then the number of literals added to B by the abstraction, decomposition, and closure rules is bounded by

$\mathcal{O}((n+k)^2)$. Indeed, since k can be considered as a constant, the numbers of added literals is bounded by $\mathcal{O}(n^2)$. It follows that the size of B is polynomially bounded by the size of Γ'. ■

9 Dense orders

Let $\Sigma_{\mathbb{O}}$ be the signature containing only the binary predicate symbol $<$ (*less than*). The theory $T_{\mathbb{O}}$ of dense order (without endpoints) is defined by the following $\Sigma_{\mathbb{O}}$-sentences:

$$
\begin{array}{ll}
(\forall x)\neg[x < x] & \text{(irreflexivity)}\\
(\forall x)(\forall y)(\forall z)[x < y \;\wedge\; y < z \;\rightarrow\; x < z] & \text{(transitivity)}\\
(\forall x)(\forall y)[x < y \;\vee\; x = y \;\vee\; y < x] & \text{(trichotomy)}\\
(\forall x)(\forall y)[x < y \;\rightarrow\; (\exists z)[x < z \;\wedge\; z < y]] & \text{(density)}\\
(\forall x)(\exists y)[y < x] & \text{(no first element)}\\
(\forall x)(\exists y)[x < y] & \text{(no last element).}
\end{array}
$$

The satisfiability problems of $T_{\mathbb{O}}$ is decidable, a result proved by Langford [6].

In this section we show that C-tableaux provide a decidability result when combining theories that share the theory $T_{\mathbb{O}}$ of dense orders. We will see that this decidability result holds despite the fact that $T_{\mathbb{O}}$ is not universal.

Let T_i be a Σ_i-theory extending the theory $T_{\mathbb{O}}$ of dense orderings, for $i = 1, 2$. In other words, we have

$$
\begin{aligned}
T_1 &= T_{\mathbb{O}} \cup S_1\,,\\
T_2 &= T_{\mathbb{O}} \cup S_2\,,
\end{aligned}
$$

for some sets of sentences S_1, S_2. Assume that $\Sigma_1 \cap \Sigma_2 = \{<\}$. In this case, C-tableaux can be made terminating without sacrificing completeness if we employ the following restrictions.

> **Restriction R1.** All rule applications must be *regular*, that is, an application of a rule R to a branch B is forbidden if it would add a literal already occurring in B.
>
> **Restriction R3.** An application of the abstraction rule to a branch B is allowed to add a literal $t = w$ only if:
>
> - t is not a variable;
> - t already occurs in B.

We now prove that, by using Restrictions R1 and R3, C-tableaux are sound, complete, and terminating, thus obtaining a decidability result when combining theories that share the dense orders.

Proposition 33 (Termination). *Using Restrictions R1 and R3, C-tableaux are terminating.* □

Proof. Let $\Gamma = \Gamma_1 \cup \Gamma_2$ be a conjunction of literals in separate form, and let T be a C-tableau obtained by exhaustively applying, subject to restrictions R1 and R3, the rules in Figure 1 to an initial C-tableau for Γ. We want to show that T is finite.

Because of restriction R3, and since the decomposition and closure rules never add a new term to T, it follows that the number of new variables introduced by the abstraction rule is finite. Therefore, every rule can be applied only a finite number of times, which implies that all branches in T are finite. Thus, T must be finite. ∎

Since C-tableaux are already sound without Restrictions R1 and R3, they are also sound with the restrictions.

Proposition 34 (Soundness). *Let $\Gamma = \Gamma_1 \cup \Gamma_2$ be a conjunction of $(\Sigma_1 \cup \Sigma_2)$-literals. Assume that there exists a closed C-tableau for Γ constructed using the rules in Figure 1 and the restrictions R1 and R3. Then Γ is $(T_1 \cup T_2)$-unsatisfiable.* □

In the forthcoming completeness proof, we will use the following proposition, which can be proved using a back-and-forth argument due to Hausdorff [3].[5]

Proposition 35. *Let $\mathcal{A}$ and $\mathcal{B}$ be two enumerable $T_{\mathbb{O}}$-interpretations. Then $\mathcal{A} \cong \mathcal{B}$.* □

Proposition 36. *Let B be an open branch of a C-tableau T. Assume that B is saturated with respect to the rules in Figure 1 and the restrictions R1 and R3. Then B is $(T_1 \cup T_2)$-satisfiable.* □

Proof. Let $V = vars(\mathsf{B})$, and let θ_i be the set of Σ_i-literals occurring in B, for $i = 1, 2$. Note that $\mathsf{B} = \theta_1 \cup \theta_2$, and that V is finite.

Since B is open, there exist a T_1-interpretation $\mathcal{A}$ satisfying θ_1 and a T_2-interpretation $\mathcal{B}$ satisfying θ_2. Without loss of generality, we can assume that A and B are enumerable, that is, $|A| = |B| = \aleph_0$.

Our goal is to merge the interpretations $\mathcal{A}$ and $\mathcal{B}$ into a $(T_1 \cup T_2)$-interpretation $\mathcal{F}$ satisfying $\theta_1 \cup \theta_2$. This goal can be accomplished by an application of the Combination Theorem 14 if we can show that $\mathcal{A}^{\{<\},V} \cong \mathcal{B}^{\{<\},V}$.

Let us define a map $f : V^{\mathcal{A}} \to V^{\mathcal{B}}$ by letting

$$f(x^{\mathcal{A}}) = x^{\mathcal{B}}\,, \qquad\qquad \text{for each } x \in V\,.$$

By saturation with respect to the decomposition rules, f is a bijective function preserving the ordering $<$. In other words, $|V^{\mathcal{A}}| = |V^{\mathcal{B}}|$ and $a <^{\mathcal{A}} b$ if and only if $f(a) <^{\mathcal{B}} f(b)$, for each $a, b \in V^{\mathcal{A}}$.

[5] In literature, Hausdorff's back and forth argument has customarily been attributed to Cantor. A recounting of this mis-attribution was written by Silver [9].

Let $a_1, a_2, \ldots, a_m$ be, in increasing order, the elements of $V^{\mathcal{A}}$. Likewise, let $b_1, b_2, \ldots, b_m$ be, in increasing order, the elements of $V^{\mathcal{B}}$. Then $f(a_i) = b_i$, for each $i = 1, \ldots, m$.

Consider the open intervals

$$(-\infty, a_1) = \{a \in A \mid a < a_1\}$$

and

$$(-\infty, b_1) = \{b \in B \mid b < b_1\} .$$

Since both intervals are $T_{\mathbb{O}}$-interpretations, by Proposition 35 there exists a bijective map

$$g_{-\infty} : (-\infty, a_1) \to (-\infty, b_1)$$

such that $a <^{\mathcal{A}} b$ if and only if $g_{-\infty}(a) <^{\mathcal{B}} g_{-\infty}(b)$, for all $a, b \in (-\infty, a_1)$. Similarly, if we let

$$(a_m, +\infty) = \{a \in A \mid a_m < a\}$$

and

$$(b_m, +\infty) = \{b \in B \mid b_m < b\}$$

then there exists a bijective map

$$g_{+\infty} : (a_m, +\infty) \to (b_m, +\infty)$$

such that $a <^{\mathcal{A}} b$ if and only if $g_{+\infty}(a) <^{\mathcal{B}} g_{+\infty}(b)$, for all $a, b \in (a_m, +\infty)$. Finally, if we let

$$(a_i, a_{i+1}) = \{a \in A \mid a_i < a < a_{i+1}\}$$

and

$$(b_i, b_{i+1}) = \{b \in B \mid b_i < b < b_{i+1}\} ,$$

for each $i = 1, \ldots, m-1$, then there exist bijective maps

$$g_i : (a_i, a_{i+1}) \to (b_i, b_{i+1})$$

such that $a <^{\mathcal{A}} b$ if and only if $g_i(a) <^{\mathcal{B}} g_i(b)$, for all $a, b \in (a_i, a_{i+1})$.

Define a map $h : A \to B$ by letting

$$h(a) = \begin{cases} f(a) , & \text{if } a = a_i \text{ , for some } i \in \{1, \ldots, m\} , \\ g_{-\infty}(a) & \text{if } a < a_1 , \\ g_{+\infty}(a) & \text{if } a_m < a , \\ g_i(a) & \text{if } a_i < a < a_{i+1} \text{ , for some } i \in \{1, \ldots, m-1\} . \end{cases}$$

Then h is an isomorphism of $\mathcal{A}^{\{<\},V}$ into $\mathcal{B}^{\{<\},V}$. ■

Proposition 37 (Completeness). *Let $\Gamma = \Gamma_1 \cup \Gamma_2$ be a conjunction of literals in separate form. If Γ is $(T_1 \cup T_2)$-unsatisfiable then there exists a closed C-tableaux T for Γ constructed using the rules in Figure 1 and the restrictions R1 and R3.* □

PROOF. Assume that Γ is $(T_1 \cup T_2)$-unsatisfiable, and let T be a C-tableau obtained by exhaustively applying, subject to the restrictions R1 and R3, the rules in Figure 1 to an initial C-tableau for Γ.

If T were not closed, then T must contain an open branch that is saturated with respect to the rules in Figure 1 and the restrictions R1 and R3. By Proposition 36, B is $(T_1 \cup T_2)$-satisfiable, which implies that Γ is also $(T_1 \cup T_2)$-satisfiable, a contradiction. ■

Combining Propositions 33, 34, and 37, we obtain the following decidability result.

Theorem 38 (Decidability). *Let T_i be a Σ_i-theory, for $i = 1, 2$, and let $\Sigma_1 \cap \Sigma_2 = \{<\}$. Assume that T_1 and T_2 are both extensions of the theory $T_{\mathbb{Q}}$ of dense order. Finally, assume that the quantifier-free satisfiability problems of T_1 and T_2 are decidable.*

Then the quantifier-free satisfiability problem of $T_1 \cup T_2$ is decidable. □

We conclude this section by proving the following complexity result.

Theorem 39 (Complexity). *Let T_i be a Σ_i-theory, for $i = 1, 2$, and let $\Sigma_1 \cap \Sigma_2 = \{<\}$. Assume that T_1 and T_2 are both extensions of the theory $T_{\mathbb{Q}}$ of dense order. Finally, assume that the quantifier-free satisfiability problems of T_1 and T_2 are decidable.*

Then the quantifier-free satisfiability problem of $T_1 \cup T_2$ is $\mathcal{NP}$-complete. □

PROOF. We can use the same argument as in the proof of Theorem 39. Consequently, let Γ be a conjunction of literals in separate form, and let B be an open branch of a C-tableau T for Γ that is saturated with respect to the rules in Figure 1 and the restrictions R1 and R3. $\mathcal{NP}$-completeness follows if we can show that the size of B is polynomially bounded by the size of Γ.

Let n be the number of terms occurring in Γ. Then the number of literals added by the abstraction, decomposition, and closure rules is bounded by $\mathcal{O}(n^2)$. It follows that the size of B is polynomially bounded by the size of Γ. ■

10 Exploiting stable finiteness

In this section we show that C-tableaux help obtaining a decidability result for a large class of combination of theories. Specifically, we are interested in combining theories T_1, T_2 such that:

(i) T_i is a universal Σ_i-theory with a decidable quantifier-free satisfiability problem, for $i = 1, 2$;

(ii) $\Sigma_1 \cup \Sigma_2$ is finite;

Input: a conjunction $\Gamma_1 \cup \Gamma_2$ of literals in separate form
Output: `succeed` if $\Gamma_1 \cup \Gamma_2$ is $(T_1 \cup T_2)$-satisfiable, and no termination otherwise

1: $V_1 \leftarrow \mathit{vars}(\Gamma_1)$
2: $V_2 \leftarrow \mathit{vars}(\Gamma_2)$
3: $V \leftarrow V_1 \cap V_2$
4: $k \leftarrow 0$
5: **while** *true* **do**
6: $\quad k \leftarrow k + 1$
7: $\quad$ **for** all $(\Sigma_1 \cup \Sigma_2)$-interpretations $\mathcal{A}$ over V such that $|A| = k$ **do**
8: $\quad\quad \mathcal{A}_1 \leftarrow \mathcal{A}^{\Sigma_1, V_1}$
9: $\quad\quad \mathcal{A}_2 \leftarrow \mathcal{A}^{\Sigma_2, V_2}$
10: $\quad\quad$ **if** $\Gamma_1 \cup \mathit{diagram}(\mathcal{A}_1)$ is T_1-satisfiable **and** $\Gamma_2 \cup \mathit{diagram}(\mathcal{A}_2)$ is T_2-satisfiable **then**
11: $\quad\quad\quad$ **return** `succeed`

The notation $\mathit{diagram}(\mathcal{A})$ in line 10 stands for a set of literals that can be intuitively seen as a finite specification of the interpretation $\mathcal{A}$. More in detail, $\mathit{diagram}(\mathcal{A})$ is effectively constructed from $\mathcal{A}$ using the following process:

1. For each element a in A, generate a fresh variable y_a. Also, initially let
$$\Delta = \{ y_a \neq y_b \mid a, b \in A \text{ and } a \neq b \}\,.$$
2. For each variable or constant symbol u in $V \cup \Sigma^{\mathrm{C}}$, if $u^{\mathcal{A}} = a$, add the literal $u = y_a$ to Δ.
3. For each function symbol f in Σ^{F} of arity n, if $a = f^{\mathcal{A}}(a_1, \ldots, a_n)$, add the literal $y_a = f(y_{a_1}, \ldots, y_{a_n})$ to Δ.
4. For each predicate symbol P in Σ^{P} of arity n, if $(a_1, \ldots, a_n) \in P^{\mathcal{A}}$, add the literal $P(y_{a_1}, \ldots, y_{a_n})$ to Δ; if instead $(a_1, \ldots, a_n) \notin P^{\mathcal{A}}$, add the literal $\neg P(y_{a_1}, \ldots, y_{a_n})$ to Δ.

We define $\mathit{diagram}(\mathcal{A})$ as the set Δ obtained at the end of this process.

Figure 5: A semi-decision procedure for the quantifier-free satisfiability problem of a stably finite theory $T_1 \cup T_2$.

(iii) $T_1 \cup T_2$ is stably finite.

If conditions (i)–(iii) are satisfied then the quantifier-free satisfiability problem of $T_1 \cup T_2$ is decidable. This decidability result can be obtained by running C-tableaux in parallel with the procedure in Figure 5. Note that decidability follows by the fact that C-tableaux are a semi-decision procedure that is sound and complete for the quantifier-free *unsatisfiability* problem of $T_1 \cup T_2$, whereas the procedure in Figure 5 is a semi-decision procedure sound and complete for the quantifier-free *satisfiability* problem of $T_1 \cup T_2$.

The following propositions prove that the procedure in Figure 5 is sound and complete for the quantifier-free satisfiability problem of $T_1 \cup T_2$.

Proposition 40. *Let $\mathcal{A}$ be a Σ-interpretation over a set V of variables, and let Φ be a set of Σ-formulae over V. Assume that $\Phi \cup \mathit{diagram}(\mathcal{A})$ is satisfiable. Then $\mathcal{A}$ satisfies $\Phi \cup \mathit{diagram}(\mathcal{A})$.* □

PROOF. Let $\mathcal{B}$ be a Σ-interpretation over V satisfying $\Phi \cup \mathit{diagram}(\mathcal{A})$. If we prove that there exists an embedding of $\mathcal{A}$ into $\mathcal{B}$, then by Proposition 4 we obtain that also $\mathcal{A}$ satisfies $\Phi \cup \mathit{diagram}(\mathcal{A})$.

Indeed, it is easy to verify that an embedding of $\mathcal{A}$ into $\mathcal{B}$ is provided by the function $h : A \to B$ defined by

$$h(a) = y_a^{\mathcal{B}}\,, \qquad \text{for each } a \in A\,. \qquad \blacksquare$$

Proposition 41 (Soundness). *Let $\Gamma = \Gamma_1 \cup \Gamma_2$ be a conjunction of literals in separate form. If the procedure in Figure 5 outputs* `succeed` *on input Γ then Γ is $(T_1 \cup T_2)$-satisfiable.* $\square$

PROOF. Assume that the procedure in Figure 5 outputs `succeed` on input $\Gamma_1 \cup \Gamma_2$.

Then there exists a finite $(\Sigma_1 \cup \Sigma_2)$-interpretation $\mathcal{A}$ such that $\Gamma_1 \cup \mathit{diagram}(\mathcal{A}_1)$ is T_1-satisfiable and $\Gamma_2 \cup \mathit{diagram}(\mathcal{A}_2)$ is T_2-satisfiable, where $\mathcal{A}_1 = \mathcal{A}^{\Sigma_1, V_1}$ and $\mathcal{A}_2 = \mathcal{A}^{\Sigma_2, V_2}$.

By Proposition 40, it follows that $\mathcal{A}_1$ satisfies $T_1 \cup \Gamma_1 \cup \mathit{diagram}(\mathcal{A}_1)$ and $\mathcal{A}_2$ satisfies $T_2 \cup \Gamma_2 \cup \mathit{diagram}(\mathcal{A}_2)$. Next, note that $\mathcal{A}_1^{\Sigma_1 \cap \Sigma_2, V_1 \cap V_2} = \mathcal{A}_2^{\Sigma_1 \cap \Sigma_2, V_1 \cap V_2} = \mathcal{A}^{\Sigma_1 \cap \Sigma_2, V_1 \cap V_2}$. Therefore, we can apply the Combination Theorem 14, and deduce that $T_1 \cup T_2 \cup \Gamma_1 \cup \Gamma_2 \cup \mathit{diagram}(\mathcal{A}_1) \cup \mathit{diagram}(\mathcal{A}_2)$ is satisfiable, which implies that $\Gamma_1 \cup \Gamma_2$ is $(T_1 \cup T_2)$-satisfiable. $\blacksquare$

Proposition 42 (Completeness). *Let $\Gamma = \Gamma_1 \cup \Gamma_2$ be a conjunction of literals in separate form. If Γ is $(T_1 \cup T_2)$-satisfiable then the procedure in Figure 5 outputs* `succeed`. $\square$

PROOF. Assume that $\Gamma_1 \cup \Gamma_2$ is $(T_1 \cup T_2)$-satisfiable. Since $T_1 \cup T_2$ is stably finite, there exists a positive integer $k > 0$ and a finite $(T_1 \cup T_2)$-interpretation $\mathcal{A}$ satisfying $\Gamma_1 \cup \Gamma_2$ such that $|A| = k$. Let $\mathcal{A}_1 = \mathcal{A}^{\Sigma_1, V_1}$. By construction of $\mathit{diagram}(\mathcal{A}_1)$, we have that $\mathcal{A}_1$ is a T_1-interpretation satisfying $\Gamma_1 \cup \mathit{diagram}(\mathcal{A}_1)$. Similarly, if we let Let $\mathcal{A}_2 = \mathcal{A}^{\Sigma_2, V_2}$ then we have that $\mathcal{A}_2$ is a T_2-interpretation satisfying $\Gamma_2 \cup \mathit{diagram}(\mathcal{A}_2)$. It follows that the procedure stops no later than at iteration k. $\blacksquare$

Summing up, we proved the following decidability result.

Theorem 43. *Let Σ_1 and Σ_2 be finite signatures, and let T_i be a universal Σ_i-theory with a decidable quantifier-free satisfiability problem, for $i = 1, 2$. Assume that $T_1 \cup T_2$ is stably finite.*

Then the quantifier-free satisfiability problem of $T_1 \cup T_2$ is decidable. $\square$

11 Conclusion

We presented C-tableaux, an extension of Smullyan tableaux for combining decision procedures for arbitrary universal theories. Given two universal theories T_1, T_2, we showed that C-tableaux are sound and complete for the *unsatisfiability* of quantifier-free formulae in the combined theory $T_1 \cup T_2$.

In general, C-tableaux are not terminating. Nevertheless, we described two approaches for obtaining decidability result using C-tableaux.

The first approach consists of employing, depending upon the specific component theories at hand, suitable restrictions to the tableau rules that enforce termination without sacrificing completeness. Using this approach, we showed that C-tableaux provide a decidability result when combining theories that share the dense orders.

The second approach consists of running in parallel with C-tableaux a semi-decision procedure that is sound and complete for the *satisfiability* of quantifier-free formulae in $T_1 \cup T_2$. Using the second approach, we were able to obtain a decidability result when we combine universal theories T_1, T_2 whose union $T_1 \cup T_2$ is stably finite.

References

[1] Melvin C. Fitting. *First-Order Logic and Automated Theorem Proving*. Graduate Texts in Computer Science. Springer, 2nd edition, 1996.

[2] Silvio Ghilardi. Quantifier elimination and provers integration. In Ingo Dahn and Laurent Vigneron, editors, *First Order Theorem Proving*, volume 86.1 of *Electronic Notes in Theoretical Computer Science*. Elsevier, 2003.

[3] Felix Hausdorff. *Grundzuege der Mengenlehre*. 1914. Reprinted in [4].

[4] Felix Hausdorff. *Grundzuege der Mengenlehre*. Chelsea Publishing Company, 1965.

[5] Wilfrid Hodges. *A Shorter Model Theory*. Cambridge University Press, 1997.

[6] C. H. Langford. Some theorems on deducibility. *Annals of Mathematics*, 28:16–40, 1927.

[7] Greg Nelson and Derek C. Oppen. Simplification by cooperating decision procedures. *ACM Transactions on Programming Languages and Systems*, 1(2):245–257, 1979.

[8] Christophe Ringeissen. Cooperation of decision procedures for the satisfiability problem. In Franz Baader and Klaus U. Schulz, editors, *Frontiers of Combining Systems*, volume 3 of *Applied Logic Series*, pages 121–140. Kluwer Academic Publishers, 1996.

[9] Charles L. Silver. Who invented Cantor's back-and-forth argument? *Modern Logic*, 4:74–78, 1994.

[10] Raymond M. Smullyan. *First-Order Logic*. Springer, 1968.

[11] Cesare Tinelli. Cooperation of background reasoners in theory reasoning by residue sharing. *Journal of Automated Reasoning*, 30(1):1–31, 2003.

[12] Cesare Tinelli and Mehdi T. Harandi. A new correctness proof of the Nelson-Oppen combination procedure. In Franz Baader and Klaus U. Schulz, editors, *Frontiers of Combining Systems*, volume 3 of *Applied Logic Series*, pages 103–120. Kluwer Academic Publishers, 1996.

[13] Cesare Tinelli and Christophe Ringeissen. Unions of non-disjoint theories and combinations of satisfiability procedures. *Theoretical Computer Science*, 290(1):291–353, 2003.

[14] Calogero G. Zarba. Combining non-disjoint theories. In Rajeev Gorè, Alexander Leitsch, and Tobias Nipkow, editors, *International Joint Conference on Automated Reasoning (Short Papers)*, Technical Report DII 11/01, pages 180–189. University of Siena, Italy, 2001.

[15] Calogero G. Zarba. A tableau calculus for combining non-disjoint theories. In Uwe Egly and Christian G. Fermüller, editors, *Automated Reasoning with Analytic Tableaux and Related Methods*, volume 2381 of *Lecture Notes in Computer Science*, pages 315–329. Springer, 2002.

[16] Calogero G. Zarba. *The Combination Problem in Automated Reasoning*. PhD thesis, Stanford University, 2004.

[17] Calogero G. Zarba, Zohar Manna, and Henny B. Sipma. Combining theories sharing dense orders. In Marta Cialdea Mayer and Fiora Pirri, editors, *Automated Reasoning with Analytic Tableaux and Related Methods: Position Papers and Tutorials*, Technical Report RT-DIA-80-2003, pages 83–98. Università di Roma Tre, Aracne Editrice, 2003.

Unité de recherche INRIA Lorraine
LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)

Unité de recherche INRIA Futurs : Parc Club Orsay Université - ZAC des Vignes
4, rue Jacques Monod - 91893 ORSAY Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier (France)
Unité de recherche INRIA Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)
Unité de recherche INRIA Sophia Antipolis : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399